When hackers cripple data, police departments pay ransom

Tewksbury, other departments powerless against computer hackers

The evil genius of ransomware is that victims are far more likely to pay small amounts to recover crucial data. REUTERS/FILE

At first, the problems with the Tewksbury Police Department system — difficulty calling up arrest and incident records — seemed to be just the usual system crankiness. No big deal.

But it persisted, and a technician was called in.

That was when the menacing message popped up on the screen, an explanation in the form of a ransom note:

“Your personal files are encrypted,” it read. “File decryption costs ~ $500.”

It continued: “If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.”

Tewksbury had joined the list of police departments victimized by “ransomware,” an insidious form of Internet crime that is crippling computers worldwide.

“My initial thoughts were we were infected by some sort of a virus,” Tewksbury Police Chief Timothy Sheehan recalled of the attack on Dec. 8. “Then we determined it was a little bit bigger than that. It was more like cyberterrorism.”

Digital thieves smuggle ransomware programs with names like KEYHolder, CryptoLocker, or CryptoWall by sending tainted e-mail messages, such as a fake notice from a package delivery service containing a hyperlink that infects the recipient’s computer when clicked.

Once on board, the ransomware program encrypts the victim’s data, making it useless without a key that unscrambles it. The victim can obtain the key by paying a ransom, usually a few hundred dollars.

The cyberattack on Tewksbury police proved so sophisticated that specialists from federal and state law enforcement agencies — plus two private Internet security firms — could not unscramble the corrupted files. After five days of desperate efforts to unlock it, Tewksbury police decided to pay the anonymous hacker the $500.

The attack was first reported over the weekend by the Tewksbury Town Crier.

Among other small-town police forces hit was the Swansea Police Department. It fell victim to the same threat in November 2013 and paid $750 to get its files back.

The police department in the Chicago suburb of Midlothian paid $500 in January. In Dickson County, Tenn., the sheriff's office came under attack in October. Despite seeking aid from the FBI, the agency ended up paying $572 in ransom.

But in Durham, N.H., Police Chief Dave Kurz chose not to pay because the department had backed up the encrypted information and could work around the seized database.

"We had to clean essentially all the computers, but all of our data was prepared," Kurz said.

The four-member police force in Collinsville, Ala., was hit in June, with the hackers demanding $500 to free up a database of mugshots. Chief Gary Bowen dug in, refused to pay, and never got his department's files back.

"There was no way we were going to succumb to what felt like terrorist threats," Bowen said.

As best as law enforcement can tell from the incidents, no data were stolen, nor were details of investigations or other sensitive police matters posted online.

The evil genius of ransomware is that victims are far more likely to pay small amounts to recover crucial data. And if enough people give in, the total can be substantial. Although the virus's success rate is unknown, a survey of CryptoLocker victims in the United Kingdom by the University of Kent found that 41 percent paid up.

"It's the old idea that if a million people give a dollar, you have a million dollars," said Diana Dolliver, a criminal justice professor at the University of Alabama who specializes in cybersecurity.

But in Detroit, hackers in April 2014 demanded the equivalent of $800,000 to unlock a city database they had encrypted. The attack became public in November, when Mayor Mike Duggan told the Detroit News the city had refused to pay because the vandalized database was not being used and did not contain critical information.

“It was a good warning sign for us,” Duggan told the newspaper.

In that case, the attackers demanded payment in bitcoin, a digital currency that is much harder to trace than other forms of money.

Moreover, in the Tewksbury case, hackers demanded that a bitcoin payment be sent through Tor, a technology that makes it very difficult to identify the physical location where the money is received.

Data security experts at Dell Inc. estimate that in a six-month period last year, CryptoWall infected more than 625,000 computers worldwide, including 250,000 in the United States. During that time, the gang that operated CryptoWall raked in about $1 million in ransom payments, according to Dell.

An earlier ransomware program, CryptoLocker, was even more profitable, hauling in between $3 million and $27 million, according to various estimates.

The Tewksbury attack revealed the hydra-like nature of some computer viruses. The Department of Justice declared last summer that an operation to disable CryptoLocker and a related virus had succeeded.

Yet other ransomware viruses have appeared in its place, doing basically the same thing.

“This is very likely a case of one of the many CryptoLocker copycats infecting police departments,” said Kyrksen Storer, spokesman for Fire Eye Inc., a Milpitas, Calif., cybersecurity firm that helped develop an online tool for retrieving files corrupted by CryptoLocker.

The Tewksbury attack featured ransomware called KEYHolder, which is designed to cover its own tracks. Tewksbury authorities sent their infected computer server to the Commonwealth Fusion Center, where Massachusetts State Police work with federal law enforcement agencies on antiterrorism and cybercrime cases. Despite their best efforts, the KEYHolder encryption proved unbreakable.

The department might have refused to pay if it had up-to-date backups of its files. Tewksbury police regularly back up their data, but those files had separately become corrupted and unusable. With no way to crack the code, Sheehan felt he had no choice but to pay to recover his original database.

Computer security analyst Brian Krebs, author of the book "Spam Nation," said it is no surprise ransomware attacks against police agencies have become public, while those against private companies have not.

"They're dealing with public funds," Krebs said. "They can't hide the fact that they paid the ransom."

Although most ransomware attacks are sent out by the thousands, Krebs warned that criminals may target specific businesses or government agencies that might be willing to pay larger sums.

"You get inside of a pharmaceutical company or something like that, that has all their net worth tied up in their files," Krebs said, "they'd be willing to pay a lot more."

Related coverage:

• 11/19/13: Swansea Police Department pays ransom to computer hackers

---

Hiawatha Bray can be reached at hiawatha.bray@globe.com.